

EXHIBIT A

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. I am also assigned to the Rhode Island Internet Crimes Against Children (ICAC) Task Force. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to, violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Kik¹ user “noahperez22” (“NOAHPEREZ22”) for distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). I submit this affidavit in support of an application to search the premises

¹ Kik, located in Santa Monica, CA, and is an instant messenger application for mobile devices, available on iOs, Android, and Windows Phone operating systems.

located at 168 Gibbs Avenue, Newport, RI 02840, (the “SUBJECT PREMISES”), as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

3. The statements in this affidavit are based in part on information provided by other HSI agents and Kik Interactive, Incorporated.

BACKGROUND OF THE INVESTIGATION

4. HSI Ottawa has been working with Kik regarding Kik users involved in possessing, receiving and/or distributing child pornography as well as Kik users involved in communications with other Kik users regarding child exploitation. Kik supplied HSI Ottawa with information on those Kik users and reported them with the following categories or ways Kik identifies those users:

a. Third-Party Moderation:

Kik uses a third-party moderation company to conduct reviews of user and group profile pictures that are uploaded. Any images found to contain child exploitation or child abuse are flagged and reported to the Trust and Safety team. The Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police and will provide:

- Subscriber data for account, in csv and pdf format
- Image

b. Support Reports:

Kik users can report illegal activity to our support team via email to support@kik.com, and if any of these incidents are found to contain child exploitation or child abuse, they are transferred to the Trust and Safety team. The Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police and will provide:

- Subscriber data for offender's account, in csv and pdf format
- Copy of the email correspondence from the reporter
- Image(s) attached by the reporter (which could be screenshots of the incident)

c. PhotoDNA Reports:

Microsoft's PhotoDNA is running on all profile picture uploads in Kik and anytime a positive hash value match is found, the Trust and Safety team is alerted. The Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police (RCMP) and will provide:

- Subscriber data, in csv and pdf format
- Image(s) flagged by the PhotoDNA service to match known child exploitation hash values

d. SafePhoto Reports:

Kik has developed an internal hash matching system (similar to PhotoDNA) with a database of approximately 92K known child

exploitation image hash values, and this system runs a hash value check against every image sent within Kik, including within private conversations. When a user sends an image with a hash value that matches a child exploitation hash value in the database, the account is banned and the Trust and Safety team receives a daily report of all positive hits. The Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police (RCMP) and will provide:

- Subscriber data of the sender, in csv format
- Log of the event(s) in csv format, including timestamp, IP address, Kik sender username, Kik receiver username (or group identifier), hash values, and event type

e. Abuse Reports:

Kik allows users to report other users who have abused or harassed them within the app. When a Kik user reports another user, they have the option to include their full conversation history, including text, and any images or videos sent between them. When our content moderators determine this content contains reference to illegal activity, a police report is generated. The Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police (RCMP) and will provide:

- Subscriber data of the reported user, in csv and pdf format

- Full conversation log that exists on the reporter's device, in word format, including timestamps and IP addresses, as well as text content
- Images/Videos associated

f. Other Reports:

Kik performs further investigations on some of the instances from the categories above. For example, if a child pornography image is sent within a group on Kik, it investigates the group's profile picture to confirm whether it is child pornography. Kik also has access to a list of current Kik users in the group, and if any appear to have explicit child pornography terms in their usernames, Kik investigates those accounts for child pornography profile pictures. If a child pornography image is found in this way, the Trust and Safety team has a mandatory obligation to report the incident to the Royal Canadian Mounted Police (RCMP) and will provide:

- Subscriber data, in csv and pdf format
- Image(s)

g. Privacy and Chat Rooms on Kik:

Kik Messenger is a free instant messaging and social networking app that uses your smartphone's data plan or Wi-Fi connection to send messages to other Kik users. It's available on iOS, Android, and Amazon for Kindle Fire. When registering with Kik, a user does not have to

provide a phone number. Kik only asks for a user's name and email address which allows a user to maintain a private presence on the platform that's identifiable only by a username, i.e., the name the user registered with. With only a username as an ID, Kik allows users to exchange messages, photos, videos, sketches, stickers, mobile webpages, emoji, and other content with others on the platform. The Kik platform appeals to individuals with privacy concerns because it allows users to remain anonymous.

A Kik user can initiate a group chat by tapping the magnifying glass search icon, tapping Start a Group, and then adding users to the group. Kik users can join a group chat, either public or private, with up to 49 other participants. Private groups are not searchable via the app and people can join by scanning the group Kik code or if they're added to the group by one of their own contacts. Public groups are searchable and identified by a hashtag. Users also have the option to directly chat with a group member, and control whether or not a user is available for direct messages.

5. HSI Ottawa, using the information received from Kik, then sent out investigative leads to HSI offices around the world. HSI Providence has received multiple leads regarding Kik users possessing, receiving and/or distributing child pornography within HSI Providence's area of responsibility.

PROBABLE CAUSE FOR KIK USER “NOAHPEREZ22”

6. In January 2020, HSI Providence received information from HSI Ottawa regarding Kik user NOAHPEREZ22. Kik reported that on August 11, 2019 at 20:54:41 UTC user NOAHPEREZ22 uploaded a video of child pornography from Internet Protocol (IP) address 72.200.189.48. The activity was reported for abuse. According to the information provided by Kik, user NOAHPEREZ22 was in a public group chat room titled “Tiny Subs” and sent the video of child pornography. I viewed the video and confirmed that the video is child pornography. The following is a description of the video uploaded to Kik by user NOAHPEREZ22:

Description: the video depicts what appears to be a partially nude, from the waist down, prepubescent female sitting with her legs spread inserting what appears to be a curling iron into her vagina.

7. Kik provided subscriber information for user NOAHPEREZ22 to include Internet Protocol (IP) logs. Using the information provided by Kik, I was able to determine that the IP addresses provided for Kik user NOAHPEREZ22 were owned by Cox Communications, Inc. (“Cox”). On February 10, 2020, an HSI administrative subpoena was served to Cox requesting subscriber information on the following IP address and which Cox customer the IP address was assigned to on the following dates and times:

IP Address: 72.200.189.48

Date/Time: 08/11/2019 @ 20:19:20 UTC

8. On March 10, 2020, Cox responded with the following subscriber information:

IP Address: 72.200.189.48

Start Date: 08/11/2019 @ 20:19:20

Stop Date: 02/08/2020 @ 00:00:00

Account Creation Date: 05/21/2013

Account Number: 1128398-09

Status: Active

Name: William Normandin

Address: 168 Gibbs Ave
Newport, RI 02840

9. On October 15, 2020, I applied for and was granted a search warrant by this court for the content of Kik account NOAHPEREZ22. I served the search warrant on Kik the same day. On October 19, 2020, Kik responded with the content from the Kik account. I reviewed the results and no content returned for the NOAHPEREZ22 account. I reviewed the logs provided by Kik and found that NOAHPEREZ22 received several messages containing files from the same Kik users who were in the “Tiny Subs” group chat platform with.

10. Based on my knowledge, training and experience, Kik users who are identified by Kik sending or receiving child exploitation material have their accounts shut down by Kik. These individuals then create new Kik accounts to continue sending and receiving child exploitation material. For example, in a previous Kik case, Kik user “mrpiff420” had his account shut down by Kik due to sending a file of child exploitation material. When agents and detectives executed a search warrant at his residence, the Kik user had created a new Kik account on his cell phone, “mrpiff4200”. In addition, in my experience, individuals such as NOAHPEREZ22 who send child pornography do so from an existing collection which they have either on their phone or some other electronic media storage account. In the past year alone, I have received approximately 15 leads from Kik, which established probable cause for search

warrants. In approximately, 12 of those leads, child pornography was found. In 1 instance, no child pornography was found at the user's residence; however in that case child pornography was located in the user's Kik account stored online. Based on my training and experience, I believe that even though NOAHPEREZ22 only distributed one child pornography file in August 2019, it is more likely than not that the user has a collection of child pornography on one or more electronic media storage devices.

11. I conducted a query of 168 Gibbs Avenue, Newport, RI 02840 using a commercial database and discovered that two individuals appear to reside at the SUBJECT PREMISES: Jodi L. (Paquin) Normandin (DOB XX/XX/1978) and William H. NORMANDIN (DOB XX/XX/1978).

12. I ran a criminal history for Jodi L. (Paquin) Normandin (DOB XX/XX/1978) and William H. NORMANDIN (DOB XX/XX/1978). Jodi Normandin's criminal history was negative. William H. NORMANDIN was convicted in 2010 for DUI and driving after denial/revocation.

13. According to online records maintained by the Newport, RI Tax Assessor, 168 Gibbs Avenue, Newport, RI 02840 is owned by Deborah D. Sieger. The SUBJECT PREMISES are described as a tan/brown one-story, ranch style home.

14. I ran an NLETS query for William and Jodi NORMANDIN's RI Driver's License (DL) information. The address listed on both RI DL's is 168 Gibbs Avenue, Newport, RI 02840.

15. The United States Postal Service (USPS) confirmed that both William and Jodi NORMANDIN are both receiving mail at 168 Gibbs Avenue, Newport, RI 02840.

16. On October 16, 2020, Newport Detective and ICAC Task Force member Joseph Lavallee conducted surveillance at the SUBJECT PREMISES. Detective Lavallee observed the number “168” affixed to the house above the front door. Detective Lavallee observed two vehicles parked at the SUBJECT PREMISES. I queried the license registration number for the vehicles (RI-117730 & RI-YN923). The vehicles are registered to William and Jodi NORMANDIN, 168 Gibbs Avenue, Newport, RI 02840.

**CHARACTERISTICS COMMON TO PERSONS WHO DISTRIBUTE,
RECEIVE, POSSESS, AND ACCESS WITH INTENT TO VIEW CHILD
PORNOGRAPHY**

17. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

18. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

19. Such offenders may collect sexually explicit or suggestive materials in a

variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

20. Such offenders almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their cache for many years.

21. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the offender's residence, inside the offender's vehicle, or, at times, on his person, to enable the individual to view the child pornography images, which are highly valued.²

22. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below,

² See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections);

evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.³

23. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography.

24. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if such an offender uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home – here, the SUBJECT PREMISES, as set forth in Attachment A.

25. In addition, I am aware, based on my training and experience and other investigations that I have conducted, that the application Kik is frequently used by individuals on their smart phones or tablet devices. These individuals tend to keep their smart phones and tablets when they move from one residence to another. Individuals who use Kik to upload and or view child pornography on Kik often have child pornography images and videos stored in their smart

³ See *United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).

phone and/or in visible in groups they are members of on Kik and other social media applications which are frequented by individuals with a sexual interest in children, often for months or years after the initial download or upload of the material. Moreover, since NOAHPEREZ22 and uploaded the video to Kik, it is necessary that NOAHPEREZ22 had the video file stored somewhere, accessible by the device used to upload it to Kik. In my training an experience, individuals with an interest in child sexual exploitation materials have more than one such video file, typically possessing many video and image files. Accordingly, it is more likely than not that NOAHPEREZ22 possesses a collection of child exploitation materials stored on or near the electronic media storage device used to access Kik, likely a smartphone or tablet.

26. Based upon the foregoing, I believe that a user of the Internet at the SUBJECT PREMISES likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. As such, I submit that there is probable cause to believe that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) exist at the SUBJECT PREMISES.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

27. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

28. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

- a. The volume of evidence: Storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect

the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

DEFINITIONS

29. For the purpose of this warrant:
- a. “Computer equipment” means any computer hardware, computer software, computer-related documentation, storage media, and data.
 - b. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
 - c. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
 - d. “Computer related documentation” means any material that explains or illustrates

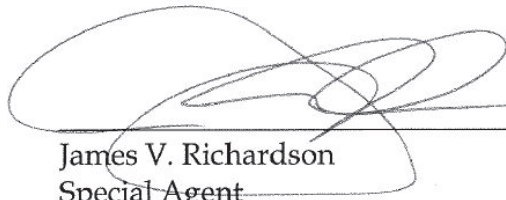
the configuration or use of any seized computer hardware, software, or related items.

- e. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- f. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- g. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

CONCLUSION

30. Based on the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (a)(4)(B), as described in Attachments B, are located at the SUBJECT PREMISES, as more fully described in Attachments A.

Respectfully submitted,


James V. Richardson
Special Agent
Homeland Security

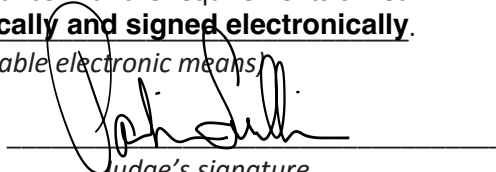
Attested to by the applicant in accordance with the requirements of Fed.
R. Crim. P. 4.1 by **Sworn telephonically and signed electronically.**
(specify reliable electronic means)

October 26, 2020

Date

Barrington, RI

City and State


Judge's signature

Patricia A. Sullivan, USMJ

Printed name and title

ATTACHMENT A

DESCRIPTION OF PERSON AND LOCATION TO BE SEARCHED

The premises to be searched include:

A. The premises located at 168 Gibbs Avenue, Newport, RI 02840, more particularly described as a tan/brown one-story, ranch style home. The number “168” is clearly affixed to the house above the front door. The exterior of the premises is pictured below:



ATTACHMENT B

DESCRIPTION OF INFORMATION TO BE SEIZED

All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2252(a)(2) and (a)(4)(B), including:

I. Records and tangible objects pertaining to the following topics:

1. Child pornography and child erotica.
2. Communications with minors or others having access to minors that relate to the persuasion, inducement, enticement or coercion of a minor to engage in sexual activity for which any person could be charged with a criminal offense.

II. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”):

1. evidence of who used, owned, or controlled the computer equipment;
2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the attachment of other computer hardware or storage media;
4. evidence of counter forensic programs and associated data that are designed to eliminate data;
5. evidence of the times the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary

to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and
8. evidence indicating the computer user's state of mind as it relates to the crime under investigation.

- III. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and
- IV. Records, information, and items relating to the ownership or use of computer equipment and other electronic storage devices found in or on the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.